Summary

Security	CVES
High	CVE-2025-71251,CVE-2025-71252,CVE-2025-71253,CVE-2025-71254,CVE-2025-71255,CVE-2025-71256

Minutia

CVE ID	CVE-2025-71251
Title	Improper Input Validation in Modem IMS
Description	In IMS, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.
Technology Area	Modem
Vulnerability Type	cwe-20 Improper Input Validation
Access Vector	Network
CVSS Rating	High
CVSS Score	7.5
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Affected Chipsets*	SC7731E/SC9832E/SC9863A/T310/T610/T618/T7200/T7225/T7250/T7255/T7280/T7300/T8100/T9100/T8200/T8300
Affected Software Versions	Android13/Android14/Android15/Android16

CVE ID	CVE-2025-71252
Title	Improper Input Validation in Modem IMS
Description	In Modem IMS, there is a possible improper input validation. This could lead to r emote denial of service with no additional execution privileges needed.
Technology Area	Modem
Vulnerability Type	CWE-20 Improper Input Validation
Access Vector	Network
CVSS Rating	High
CVSS Score	7.5
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Affected Chipsets*	SC7731E/SC9832E/SC9863A/T310/T610/T618/T7200/T7225/T7250/T7255/T72 80/T7300/T8100/T9100/T8200/T8300
Affected Software Versi ons	Android13/Android14/Android15/Android16

CVE ID	CVE-2025-71253
Title	Improper Input Validation in Modem IMS
Description	In Modem IMS, there is a possible improper input validation. This could lead to r emote denial of service with no additional execution privileges needed.
Technology Area	Modem
Vulnerability Type	CWE-20 Improper Input Validation
Access Vector	Network
CVSS Rating	High
CVSS Score	7.5
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Affected Chipsets*	SC7731E/SC9832E/SC9863A/T310/T610/T618/T7200/T7225/T7250/T7255/T72 80/T7300/T8100/T9100/T8200/T8300
Affected Software Versi ons	Android13/Android14/Android15/Android16

CVE ID	CVE-2025-71254
Title	Improper Input Validation in Modem IMS
Description	In Modem IMS, there is a possible improper input validation. This could lead to r emote denial of service with no additional execution privileges needed.
Technology Area	Modem
Vulnerability Type	CWE-20 Improper Input Validation
Access Vector	Network
CVSS Rating	High
CVSS Score	7.5
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Affected Chipsets*	SC7731E/SC9832E/SC9863A/T310/T610/T618/T7200/T7225/T7250/T7255/T72 80/T7300/T8100/T9100/T8200/T8300
Affected Software Versi ons	Android13/Android14/Android15/Android16

CVE ID	CVE-2025-71255
Title	Improper Input Validation in Modem IMS
Description	In Modem IMS, there is a possible improper input validation. This could lead to r emote denial of service with no additional execution privileges needed.
Technology Area	Modem
Vulnerability Type	CWE-20 Improper Input Validation
Access Vector	Network
CVSS Rating	High
CVSS Score	7.5
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Affected Chipsets*	SC7731E/SC9832E/SC9863A/T310/T610/T618/T7200/T7225/T7250/T7255/T72 80/T7300/T8100/T9100/T8200/T8300
Affected Software Versi ons	Android13/Android14/Android15/Android16

CVE ID	CVE-2025-71256
Title	Improper Input Validation in nr Modem
Description	In nr modem, there is a possible improper input validation. This could lead to rem ote denial of service with no additional execution privileges needed.
Technology Area	Modem
Vulnerability Type	CWE-20 Improper Input Validation
Access Vector	Network
CVSS Rating	High
CVSS Score	7.5
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Affected Chipsets*	T8100/T9100/T8200/T8300
Affected Software Versi ons	Android13/Android14/Android15/Android16

*The list of affected chipsets may not be complete. For latest information, device OEMs can contact directly at https://unisupport.unisoc.com

Vulnerability type definition

Abbreviation	Interpretation
RCE	Remote Code Execution
EoP	Elevation of Privilege
ID	Information Disclosure
DoS	Denial of Service
N/A	Classification not available

Version

Version	Date	Description
1.0	2026-05-06	